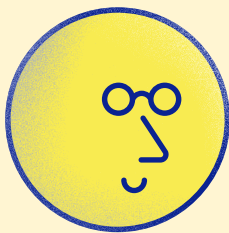


# Cara mengenal dan menghindari penipuan



Panduan Anda untuk  
melindungi diri Anda dari  
penipuan



Australian Government



National  
Anti-Scam  
Centre



**ScamWatch**  
Stop. Better safe than scammed.

## Pengakuan terhadap negara

ACCC mengakui pemilik tradisional dan penjaga Negara di seluruh Australia dan mengakui kesinambungan hubungan mereka dengan tanah, laut, dan masyarakat. Kami memberikan penghormatan kepada mereka dan budaya mereka; dan kepada Sesebuah mereka di masa lalu, sekarang, dan masa depan.

Australian Competition and Consumer Commission  
Ngunnawal  
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601  
© Persemakmuran Australia 2023

Karya ini memiliki hak cipta. Selain penggunaan apa pun yang diizinkan berdasarkan *Undang-Undang Hak Cipta 1968*, semua materi yang terkandung dalam karya ini disediakan di bawah lisensi Creative Commons Attribution 4.0 Australia, dengan pengecualian:

- Lambang Persemakmuran
- logo ACCC dan AER
- setiap ilustrasi, diagram, foto atau grafik yang hak ciptanya tidak dimiliki oleh Komisi Persaingan dan Konsumen Australia, namun mungkin menjadi bagian atau terkandung dalam publikasi ini.

Rincian ketentuan lisensi yang relevan tersedia di situs web Creative Commons, begitu pula kode hukum lengkap untuk lisensi CC BY 4.0 AU.

Permintaan dan pertanyaan mengenai reproduksi dan hak harus ditujukan kepada Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

### Pemberitahuan Penting

Informasi dalam publikasi ini hanya untuk panduan umum. Informasi ini tidak merupakan nasihat hukum atau nasihat profesional lainnya, dan jangan diandalkan sebagai pernyataan hukum di yurisdiksi mana pun. Karena dimaksudkan hanya sebagai panduan umum, maka mungkin berisi generalisasi. Anda harus mendapatkan nasihat profesional jika Anda mempunyai kekhawatiran khusus.

ACCC telah melakukan segala upaya yang wajar untuk memberikan informasi terkini dan akurat, namun ACCC tidak memberikan jaminan apa pun mengenai keakuratan, kekinian, atau kelengkapan informasi tersebut.

Pihak-pihak yang ingin menerbitkan kembali atau menggunakan informasi dalam publikasi ini harus memeriksa kebaruan dan keakuratan informasi ini sebelum diterbitkan. Hal ini harus dilakukan sebelum setiap edisi publikasi, karena pedoman ACCC dan undang-undang transisi yang relevan sering berubah. Pertanyaan apa pun yang dimiliki setiap pihak harus ditujukan kepada Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24\_24-13

[www.accc.gov.au](http://www.accc.gov.au)

# Daftar Isi

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>Bantuan tersedia</b>                                                   | <b>1</b>  |
| <b>Apa itu penipuan (scam)</b>                                            | <b>3</b>  |
| <b>Langkah-langkah sederhana untuk mengenali dan menghindari penipuan</b> | <b>4</b>  |
| <b>Penipuan pesan atau SMS</b>                                            | <b>7</b>  |
| <b>Penipuan email</b>                                                     | <b>11</b> |
| <b>Penipuan panggilan telepon</b>                                         | <b>15</b> |
| <b>Penipuan situs web</b>                                                 | <b>19</b> |
| <b>Penipuan di media sosial, berbasis aplikasi, dan pemesanan online</b>  | <b>23</b> |
| <b>Penipuan teratas yang harus Anda ketahui</b>                           | <b>27</b> |
| <b>Ke mana melaporkan penipuan</b>                                        | <b>31</b> |
| <b>Lebih banyak bantuan dan dukungan</b>                                  | <b>33</b> |



## Panduan ini ditulis oleh National Anti-Scam Center dan akan membantu Anda mengidentifikasi dan melindungi diri Anda dari bahaya yang disebabkan oleh penipuan.

Penipuan adalah kejahatan dan orang yang melakukan penipuan adalah penjahat. Banyak orang di Australia kena tipu dan kehilangan uang, bahkan terkadang tabungan seumur hidup mereka. Penipuan merugikan kehidupan banyak orang.

Penipuan semakin sulit dikenali, jadi kita perlu bekerja sama untuk menghentikannya.

National Anti-Scam Centre berupaya menjaga warga Australia aman dari penipuan.

Kami bekerja sama dengan pemerintah dan industri untuk menemukan cara baru menghentikan para penipu mencuri uang dan informasi pribadi warga Australia. Berikut adalah beberapa cara kami mencapai hal ini.

### **Kami membantu orang mengenali dan menghindari penipuan**

Melalui Scamwatch kami berbagi informasi terkini tentang penipuan dan cara melindungi diri Anda dari penipuan.

### **Kami mengganggu para penipu (scammers)**

Dengan mengumpulkan dan membagikan informasi intelijen ke seluruh pemerintahan dan industri, kami mempersulit para penipu untuk melanjutkan kejahatan mereka dan memudahkan masyarakat untuk melaporkan penipuan.



# Bantuan tersedia

Jika Anda membaca ini, kemungkinan besar Anda, atau seseorang yang Anda kenal telah kena tipu. Sayangnya, Anda tidak sendirian. Penipuan semakin canggih yang berarti siapa pun dapat ditipu.

Jika Anda telah ditipu, penting bahwa Anda bertindak cepat.

Jika Anda kehilangan uang karena penipuan, hubungi bank atau penyedia kartu Anda.

Hubungi IDCARE, **1800 595 160**, [www.idcare.org](http://www.idcare.org).

Penipuan berhasil karena terlihat seperti yang resmi. Penipu mengandalkan Anda untuk tidak melihat tanda-tanda peringatan karena Anda sedang terburu-buru, sesuatu yang tampaknya tidak ingin Anda lewatkan, atau karena sepertinya itu berasal dari seseorang yang Anda percayai.

## Lindungi diri Anda dari penipuan dengan mengikuti 3 langkah berikut:

### Berhenti



Jangan memberikan uang atau informasi pribadi kepada siapa pun jika tidak yakin.

Penipu akan menawarkan bantuan atau meminta Anda memverifikasi siapa Anda. Mereka akan berpura-pura berasal dari organisasi yang Anda kenal dan percayai seperti penyedia layanan, polisi, bank, atau layanan pemerintah.

### Periksa



Tanyakan pada diri Anda – apakah pesan atau panggilan tersebut palsu?

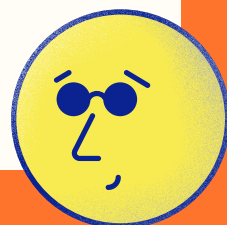
Jangan pernah mengklik tautan dalam pesan. Hanya hubungi bisnis atau pemerintah menggunakan informasi kontak yang Anda temukan dari situs web atau aplikasi resmi mereka. Jika Anda tidak yakin, katakan 'tidak', tutup panggilan atau hapus pesan.

### Laporkan



Bertindak cepat jika ada yang tidak beres.

Hubungi bank Anda jika Anda melihat aktivitas yang tidak biasa atau jika seorang penipu mendapatkan uang atau informasi Anda. Cari bantuan dan laporkan penipuan tersebut ke ReportCyber dan Scamwatch. Saat Anda melaporkan penipuan, Anda membantu seluruh warga Australia dengan membangun pertahanan kita terhadap penipuan.



# Apa itu penipuan (scam)

Penipuan adalah ketika seseorang menipu Anda untuk mencuri uang atau informasi pribadi Anda.

Penipuan adalah kejahatan ekonomi yang dilakukan oleh penjahat yang seringkali sangat terorganisir dan canggih.

## Penipuan:

-  dijalankan oleh penjahat
-  terlihat nyata
-  datang dengan cerita yang dapat dipercaya
-  menekan Anda untuk mengambil tindakan

## Penipuan BUKAN:

-  Peretasan komputer (hacking)
-  Persyaratan kontrak yang tidak adil
-  Pendekatan pemasaran yang merundung

Penting untuk diingat bahwa tidak semua pengalaman negatif adalah penipuan. Anda mungkin telah membayar untuk suatu produk tetapi Anda tidak pernah menerimanya atau membeli sesuatu dan ternyata kualitasnya buruk. Meskipun ini mengecewakan, ini belum tentu merupakan penipuan. Undang-undang Konsumen Australia menawarkan perlindungan kepada konsumen Australia atas permasalahan-permasalahan seperti ini.

Untuk informasi lebih lanjut kunjungi [www.accc.gov.au/consumers](http://www.accc.gov.au/consumers)

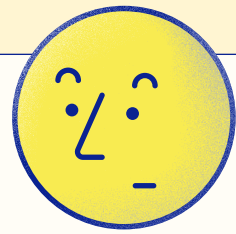
# Langkah-langkah sederhana untuk mengenali dan menghindari penipuan

Penipuan dapat terjadi pada kita semua. Penipuan berhasil karena penipu membuat cerita yang dapat dipercaya untuk mencuri uang Anda dan mendapatkan informasi pribadi Anda.

Para penipu semakin pintar dan memanfaatkan teknologi, produk, layanan, dan peristiwa besar baru untuk meyakinkan Anda bahwa penipuan mereka benar.

Sangat sulit untuk menemukan penipuan. Berikut adalah beberapa situasi yang harus diwaspadai. Terkadang penipu menggunakan kombinasi taktik ini.

- 1. Peluang untuk menghasilkan atau menghemat uang:**Penipu akan menipu Anda agar percaya bahwa Anda mendapatkan harga atau penawaran yang luar biasa. Mereka akan menekan Anda untuk bertindak cepat agar Anda tidak ketinggalan. Ingat, harga atau penawaran yang tampaknya terlalu bagus untuk menjadi kenyataan, biasanya memang demikian.
- 2. Kisah sedih dan tangisan minta tolong:**Penipu akan mencoba menggunakan sifat baik Anda untuk memanfaatkan Anda. Mereka akan berbagi cerita tentang patah hati dan tragedi dengan Anda dan menjelaskan mengapa mereka membutuhkan bantuan dan uang Anda.
- 3. Tautan dan lampiran:**Penipu menggunakan tautan (links) untuk mengirim Anda ke situs web penipuan yang dirancang untuk mencuri informasi dan uang Anda. Penipu mungkin juga meminta Anda membuka lampiran (attachment). Ini dapat menginstal virus yang mencuri informasi Anda.



4. **Tekanan untuk bertindak cepat:**Penipu tidak ingin Anda meluangkan waktu dan memikirkan semuanya. Mereka ingin menekan Anda agar bertindak cepat. Hal ini dapat mencakup ancaman bahwa sesuatu yang buruk akan terjadi jika Anda tidak bertindak cepat.
5. **Permintaan agar Anda membayar dengan cara yang tidak biasa atau spesifik:**Penipu sering kali meminta Anda membayar menggunakan metode yang tidak biasa seperti kartu debit yang sudah dimuat sebelumnya, kartu iTunes, atau mata uang virtual seperti Bitcoin. Setelah uang ini habis, Anda tidak dapat mendapatkannya kembali.
6. **Permintaan untuk membuat akun atau PayID baru:**Penipu mungkin meminta Anda membuat rekening bank atau PayID baru untuk membayar mereka (atau dibayar oleh mereka). Mereka mungkin berpura-pura menjadi bank Anda dan meminta Anda mentransfer uang Anda ke rekening baru agar tetap aman.

Jika penipu telah berhasil mengambil uang Anda, mereka akan berusaha mendapatkan lebih banyak uang dari Anda. Sayangnya, satu dari tiga korban penipuan telah kena tipu lebih dari sekali. Jika Anda telah kehilangan uang karena penipuan, waspadalah terhadap penipu yang menawarkan bantuan untuk mendapatkan uang Anda kembali. Ini merupakan jenis penipuan lanjutan lainnya.



# Penipuan pesan atau SMS

Penipu mengirim pesan dengan berpura-pura dari pemerintah, penegak hukum, bisnis terpercaya, atau bahkan keluarga atau teman Anda sendiri.

Pesan-pesan ini akan terdengar mendesak dan mencoba membuat Anda bertindak cepat. Pesan-pesan ini sering kali memiliki tautan yang akan membawa Anda ke situs web penipuan. Penipu dapat mencuri informasi pribadi apa pun yang dimasukkan ke situs penipuan ini dan menggunakannya untuk mengambil uang Anda atau melakukan penipuan atas nama Anda.

Untuk membuat pesan-pesan ini tampak resmi, penipu menyalin atau menyamarkan nomor telepon mereka di belakang nomor telepon dan ID penelepon dari bisnis sah atau orang yang Anda kenal.

Pesan penipuan bahkan dapat muncul dalam rantai pesan (message chain) yang sama dengan pesan sebenarnya dari organisasi, sehingga membuatnya semakin sulit dikenali.

## Tanda-tanda sebuah pesan mungkin merupakan penipuan

### Pesan:

---



Meminta Anda untuk segera mengambil tindakan, melakukan pembayaran, atau mentransfer uang.

---



Meminta Anda untuk mengklik tautan atau menghubungi nomor yang disediakan dalam pesan.

---



Meminta Anda untuk masuk ke akun online dengan nama pengguna dan kata sandi Anda atau untuk memberikan informasi pribadi lainnya.

---



Berasal dari anggota keluarga atau teman yang mengatakan detail kontak mereka telah berubah.

---



Mengancam akan menghentikan layanan atau menagih Anda jika Anda tidak bertindak.

---



Menyiratkan Anda atau akun Anda telah diretas atau terlibat dalam penipuan.

---



Menyiratkan bahwa ada masalah dengan pembayaran atau pengiriman paket Anda.

---

## Langkah-langkah untuk melindungi diri Anda dari penipuan perpesanan

---

1. Jika seseorang yang Anda kenal mengirim pesan yang memberitahukan bahwa mereka memiliki nomor telepon baru:



- a. coba hubungi mereka di nomor yang Anda miliki untuk mereka, dan
- b. kirim pesan kepada mereka di nomor baru dengan pertanyaan yang hanya mereka akan tahu jawabannya, untuk memastikan bahwa mereka adalah siapa yang mereka katakan.



2. Jangan pernah mengklik tautan dalam pesan.



3. Jika sebuah pesan tertaut ke suatu situs web, jangan klik tautan tersebut. Cari sendiri situs webnya secara online, atau gunakan aplikasi resmi.



4. Jangan membalas pesan teks menggunakan nomor telepon yang disediakan.



5. Hubungi kembali organisasi atau orang tersebut melalui nomor telepon yang Anda temukan sendiri, misalnya dari situs web organisasi tersebut.



# Penipuan email

Penipu mengirim email dengan berpura-pura dari pemerintah, penegak hukum, dan bisnis. Email-email tersebut terdengar mendesak agar Anda bertindak cepat.

Penipu menggunakan logo yang sama dan alamat email yang serupa dengan organisasi sebenarnya. Penipu juga dapat menyalin atau menyamarkan alamat email mereka di belakang alamat email organisasi atau bisnis untuk membuat email penipuan terlihat lebih resmi.

## Tanda-tanda email mungkin merupakan penipuan

### Email tersebut:

---



Meminta pembayaran tetapi detail akunnya baru atau telah berubah sejak pembayaran terakhir yang Anda lakukan.

---



Meminta Anda untuk masuk ke akun online dengan nama pengguna dan kata sandi Anda atau untuk memberikan informasi pribadi lainnya.

---



Tidak terduga dan menyertakan lampiran dengan undangan untuk membukanya.

---



Meminta Anda mengonfirmasi detail perbankan Anda untuk menerima pengembalian dana atau uang yang tidak Anda harapkan.

---



Mengaku mempunyai informasi tentang Anda atau foto Anda dan mengancam akan menyebarkannya.

---



Menawarkan untuk membantu Anda mendapatkan uang kembali atau mendapatkan kompensasi atas pelanggaran data atau pencurian identitas.

---

# Langkah-langkah yang dapat Anda ambil untuk melindungi diri Anda dari penipuan email

---

1. Periksa apakah email tersebut resmi dengan:



- a. menghubungi orang atau organisasi tersebut secara langsung menggunakan rincian kontak yang Anda temukan seperti dari situs web organisasi atau,
  - b. mengakses organisasi melalui aplikasi resmi mereka (jangan pernah melalui tautan).
- 



2. Segera hentikan kontak dengan siapa pun yang mencoba mengancam atau mengintimidasi Anda.
- 

3. Jangan pernah memberikan rincian pribadi atau membayar siapa pun yang menawarkan kepada Anda:



- a. kompensasi atau bantuan untuk mendapatkan kembali dari penipuan atau pelanggaran data sebelumnya atau,
  - b. kemenangan, hadiah atau warisan.
- 

4. Gunakan autentikasi multifaktor bila memungkinkan. Ini memberikan lapisan perlindungan ekstra dan berarti penipu harus mengetahui kata sandi email Anda dan nomor pin yang dikirimkan ke ponsel Anda untuk mendapatkan akses ke akun email Anda.
- 





# Penipuan panggilan telepon

Penipu menelepon, mengaku berasal dari organisasi terkenal. Ini termasuk organisasi pemerintah, penegak hukum, firma hukum dan investasi, bank, dan penyedia telekomunikasi.

Mereka membuatnya terdengar mendesak agar Anda bertindak cepat. Mereka mungkin mencoba meyakinkan Anda untuk memberikan rincian pribadi atau rekening bank Anda, atau akses ke komputer Anda.

Penelepon mungkin sudah mengetahui beberapa detail tentang Anda, seperti nama atau alamat Anda, sehingga panggilan tersebut tampak benar.

## Tanda-tanda panggilan telepon mungkin penipuan

### Penelepon:

---



Meminta pembayaran atau meminta Anda memindahkan uang ke rekening baru.

---



Meminta kata sandi, pin, kode sekali pakai, atau informasi keamanan lainnya.

---



Meminta detail keuangan Anda, seperti detail kartu kredit atau perbankan.

---



Meminta Anda menyelesaikan suatu tindakan di ponsel atau komputer Anda seperti menginstal perangkat lunak atau mengakses akun aman.

---



Mengaku berasal dari penegak hukum dan mengancam Anda dengan penangkapan atau deportasi segera.

---



Mengatakan bank Anda atau rekening daring lainnya telah diretas atau terlibat dalam penipuan.

---

# Langkah-langkah yang dapat Anda ambil untuk melindungi diri Anda dari penipuan panggilan telepon

1. Periksa apakah panggilan tersebut benar dengan:



- a. menghubungi orang atau organisasi tersebut secara langsung menggunakan rincian kontak yang Anda temukan seperti dari situs web organisasi atau,
- b. mengakses organisasi melalui aplikasi resmi mereka (jangan pernah melalui tautan).



2. Jika Anda tidak yakin siapa peneleponnya atau apakah mereka mengancam atau mengintimidasi Anda, segera tutup panggilan itu.



3. Jangan pernah menginstal perangkat lunak yang mengizinkan seseorang mengakses komputer atau perangkat Anda.



4. Anda dapat mengabaikan panggilan dari nomor yang tidak Anda kenal atau membiarkan panggilan itu masuk ke pesan suara.



## Penting untuk diketahui!

Anda masih dapat menerima panggilan penipuan meskipun Anda memiliki nomor privat atau terdaftar dalam daftar Jangan Panggil (Do Not Call).



# Penipuan situs web

Penipu dapat berpura-pura menjadi siapa saja yang sedang online, termasuk pemerintah, pelaku bisnis, selebriti, atau teman atau keluarga Anda.

Mereka dapat membuat situs web palsu agar terlihat seperti merek terkenal. Mereka mungkin meniru orang-orang terkenal dan membuatnya tampak seperti mereka menyetujui suatu barang atau jasa. Situs web ini mungkin berisi ulasan palsu untuk membuat Anda memercayainya.

Anda mungkin melihat spanduk iklan palsu atau jendela pop-up yang berisi peringatan palsu atau pesan kesalahan saat online.

## Tanda-tanda sebuah situs web mungkin merupakan penipuan

Situs web itu:

---



Menawarkan barang untuk dijual dengan harga yang jauh lebih rendah dari biasanya atau dibandingkan dengan situs lain.

---



Memberi tahu Anda cara menghasilkan uang dengan cepat dan mudah dengan sedikit risiko atau usaha.

---



Berisi peringatan mendesak atau pesan kesalahan yang meminta Anda mengklik tautan.

---



Meminta pembayaran dengan cara yang tidak biasa atau spesifik seperti kartu hadiah atau mata uang kripto seperti Bitcoin.

---



Hanya mencakup ulasan positif.

---

## Langkah-langkah yang dapat Anda ambil untuk menghindari penipuan situs web



1. Membandingkan harga-harga Jika suatu tawaran tampak terlalu bagus untuk menjadi kenyataan, mungkin memang demikian.



2. Teliti organisasi atau orang yang berurusan dengan Anda sebelum memberikan uang atau informasi pribadi Anda.



3. Jangan mengandalkan ulasan yang ditulis di situs web itu sendiri. Telusuri situs web atau nama bisnis dan kata 'scam' (penipuan) atau 'reviews' (ulasan).



4. Jika peringatan atau pesan kesalahan (error message) muncul di layar Anda, jangan klik pesan tersebut, melainkan buka langsung aplikasi yang dirujuknya untuk memeriksa apakah itu benar.



5. Selalu perbarui perangkat yang Anda gunakan untuk belanja online dengan mengaktifkan 'pembaruan otomatis' untuk sistem operasi dan aplikasi Anda.



### Penting untuk diketahui!

Cara-cara praktis untuk melindungi diri Anda secara online tersedia di [www.cyber.gov.au](http://www.cyber.gov.au)



# Penipuan media sosial, berbasis aplikasi, dan perpesanan online

Jika seseorang yang tidak Anda kenal menghubungi Anda di media sosial, platform perpesanan seperti WhatsApp atau WeChat, atau melalui aplikasi, bisa jadi itu adalah penipuan.

Penipu yang berpura-pura menjadi orang lain sering kali menggunakan foto asli orang tersebut atau logo resmi organisasi yang mereka pura-pura menjadi orang lain, agar membuat penipuan lebih sulit dikenali.

Penipu di media sosial akan membuat profil palsu dan berpura-pura berasal dari pemerintah, bisnis resmi, pemberi kerja, perusahaan investasi, atau bahkan teman, anggota keluarga, atau kekasih.

Mereka mungkin menyamar sebagai orang terkenal dan membuatnya tampak seperti sedang mempromosikan barang atau jasa.

Penipu juga dapat mengetahui banyak tentang Anda dari detail yang Anda bagikan di akun media sosial Anda. Mereka dapat menggunakan informasi ini untuk menebak kata sandi akun Anda atau menargetkan Anda dengan penipuan lainnya.

## Tanda-tanda penipuan media sosial atau aplikasi

### Profil media sosial atau aplikasi:

---



Memberi tahu Anda cara menghasilkan uang dengan cepat dan mudah dengan sedikit risiko atau usaha.

---



Mengundang Anda untuk mengikuti kompetisi atau penawaran waktu terbatas.

---



Meminta untuk memindahkan percakapan dari aplikasi seperti aplikasi kencan ke obrolan pribadi atau email.

---



Menyiratkan orang terkenal mendukung atau mendukung suatu produk atau layanan.

---



Mengatakan bahwa seseorang lain akan membeli sesuatu yang Anda jual tanpa melihatnya terlebih dahulu dan dengan harga yang tinggi.

---



Mengancam akan membagikan foto pribadi Anda kecuali Anda membayar mereka uang.

---



Menghubungi Anda untuk menawarkan pekerjaan kepada Anda.

---



### Penting untuk diketahui!

Informasi mengenai cara tetap aman di berbagai platform media sosial dapat ditemukan di [www.esafety.gov.au](http://www.esafety.gov.au)

## Langkah-langkah yang dapat Anda ambil untuk menghindari penipuan media sosial dan penipuan berbasis aplikasi



1. Periksa apakah profil tersebut mungkin palsu. Apakah akunnya aktif? Berapa banyak teman/pengikut yang mereka miliki dan berapa banyak yang mereka posting secara online?



2. Cari nama profil online dengan kata 'scam'.



3. Jangan pernah mengambil pekerjaan yang ditawarkan kepada Anda tanpa wawancara, atau diskusi tentang pengalaman, kesesuaian, dan referensi Anda. Teliti perekrut dan bisnis atau individu yang menawarkan posisi tersebut. Hubungi agen perekrutan melalui nomor telepon yang bersumber dari pencarian internet independen. Jangan membayar uang muka hanya untuk mendapatkan pekerjaan.



4. Ikutilah saran investasi hanya dari seseorang yang memiliki izin Jasa Keuangan Australia dan periksa apakah perusahaan atau situs web tersebut tidak disebutkan dalam portal peringatan investor Organisasi Internasional Komisi Sekuritas (IOSCO).



5. Jangan pernah memberikan uang kepada orang yang hanya Anda temui secara online. Penipu sering kali mengatakan bahwa mereka tinggal di luar negeri dan tidak dapat bertemu langsung dengan Anda.



6. Jangan pernah mengirimkan foto intim diri Anda kepada seseorang yang hanya Anda temui secara online.

Untuk informasi lebih lanjut tentang penipuan termasuk cara lain penipu menghubungi Anda, seperti secara langsung dan melalui surat, kunjungi [Scamwatch](#).



# Penipuan teratas yang harus Anda ketahui

Berikut beberapa jenis penipuan paling umum yang perlu Anda waspadai. Anda dapat menemukan informasi lebih lanjut mengenai masing-masing jenis penipuan ini, termasuk tanda peringatan dan langkah-langkah untuk melindungi diri Anda, di situs web [Scamwatch](#).

## **Penipuan peniruan identitas**

Penipu menipu Anda dengan membuat Anda mengira mereka berasal dari organisasi tepercaya seperti polisi, pemerintah, bank, dan bisnis terkenal. Mereka bahkan dapat berpura-pura menjadi teman atau anggota keluarga Anda. Penipu mencari informasi tentang Anda dengan mengirimkan email atau pesan phishing. Ini dirancang untuk mencuri informasi Anda. Mereka mencoba dan meyakinkan Anda untuk memberikan informasi pribadi Anda dengan berpura-pura bahwa mereka berasal dari organisasi resmi atau seseorang yang Anda kenal dan percayai.

Penipu menggunakan teknologi untuk membuat panggilan atau pesan mereka tampak berasal dari nomor telepon yang sah. Mereka dapat membuat pesan teks muncul di jalur (thread) percakapan yang sama dengan pesan resmi dari suatu organisasi.

## **Penipuan investasi**

Penipu menggunakan pemasaran yang meyakinkan dan teknologi baru untuk membuat proposal investasi mereka terdengar terlalu sayang untuk dilewatkan. Mereka menjanjikan Anda keuntungan besar dengan sedikit atau tanpa risiko. Mereka sering kali menggunakan taktik tekanan agar Anda bertindak cepat, sehingga mereka dapat mencuri uang Anda.

## **Penipuan pekerjaan dan ketenagakerjaan**

Penipu menawarkan pekerjaan dengan gaji tinggi dengan sedikit usaha. Mereka berpura-pura merekrut atas nama perusahaan terkenal dan platform belanja online. Terkadang, pekerjaan yang mereka daftarkan bahkan tidak ada. Penipu juga menyamar sebagai agen perekrutan terkenal. Tujuan mereka adalah mencuri uang dan informasi pribadi Anda. Mereka mungkin meminta Anda membayar uang muka agar dapat bekerja untuk mereka.

## **Penipuan produk dan layanan**

Penipu berperan sebagai pembeli atau penjual untuk mencuri uang Anda. Mereka membuat situs web atau profil palsu di situs pengecer sah yang menawarkan produk atau layanan dengan harga yang terlalu bagus untuk menjadi kenyataan. Mereka memposting iklan palsu dan ulasan palsu. Mereka mungkin menggunakan logo curian, nama domain .com.au, dan Nomor Bisnis Australia (ABN) curian. Penipuan ini sulit dikenali.

Penipu juga berperan sebagai bisnis yang Anda kenal dan percaya untuk mengirimkan tagihan palsu kepada Anda. Mereka bahkan dapat mengubah detail faktur yang sah sehingga pelangganlah yang membayar si penipu, bukan Anda.

## **Penipuan romantis**

Penipu menggunakan janji cinta, kencan, atau persahabatan untuk mencuri uang Anda. Mereka berusaha keras untuk meyakinkan Anda bahwa hubungan itu nyata dan memanipulasi Anda untuk memberi mereka uang.

Penipu menemukan Anda di media sosial, aplikasi kencan atau game, dan situs web. Mereka mungkin juga mengirim SMS atau email kepada Anda. Mereka bersembunyi di balik profil dan identitas palsu, terkadang orang-orang terkenal. Begitu Anda memercayai mereka, mereka akan mengalami 'keadaan darurat' dan meminta bantuan Anda. Ini sering kali berupa permintaan uang atau produk lainnya.

## **Ancaman dan penipuan pemerasan**

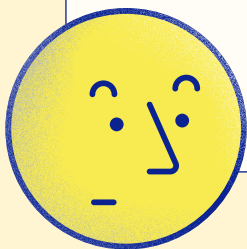
Penipu berpura-pura berasal dari organisasi tepercaya dan mengklaim Anda perlu membayar uang atau sesuatu yang buruk akan terjadi. Mereka mungkin mengancam Anda dengan penangkapan, deportasi, atau bahkan kekerasan fisik, jika Anda tidak setuju untuk segera membayarnya.

Mereka juga dapat memeras Anda dengan mengancam akan membagikan gambar atau video bugil yang Anda kirimkan kecuali jika Anda mengirimkan uang kepada mereka.

## **Penipuan uang tak terduga**

Penipu mencoba meyakinkan Anda bahwa Anda berhak atas uang atau kemenangan yang tidak Anda harapkan akan menerimanya.

Penipu meminta Anda membayar biaya atau memberikan rincian perbankan atau identitas Anda sebelum Anda dapat mengambil uang atau kemenangan. Sayangnya, tidak ada uang gratis.





# Ke mana melaporkan penipuan

Kami berupaya menjadikan Australia sebagai target yang lebih sulit bagi para penipu dengan meningkatkan kesadaran tentang cara mengenali, menghindari, dan melaporkan penipuan.

Kami berbagi informasi dari laporan penipuan dan bekerja sama dengan pemerintah, penegak hukum, dan sektor swasta untuk mengganggu dan mencegah penipuan.

Bantu orang lain dengan melaporkan ke Scamwatch. Laporkan pengalaman penipuan Anda melalui formulir laporan di situs web Scamwatch [www.scamwatch.gov.au](http://www.scamwatch.gov.au)

Ingat, jika Anda adalah korban penipuan, penting bagi Anda untuk bertindak cepat.

- Jika Anda kehilangan uang karena penipu, hubungi bank atau penyedia kartu Anda.
- Hubungi ID CARE: 1800 595 160 | [idcare.org](http://idcare.org)



# Lebih banyak bantuan dan dukungan

Menjadi korban penipuan dapat membuat Anda kewalahan. Penting untuk diingat bahwa hal ini dapat terjadi pada siapa saja, dan tersedia dukungan.

Jika Anda atau seseorang yang Anda kenal telah kena tipu, bicarakan dengan seseorang tentang hal itu. Anda dapat mencari dukungan dari keluarga, teman, dokter umum Anda atau salah satu layanan dukungan berikut.

**Lifeline: 13 11 14 | [lifeline.org.au](https://lifeline.org.au)**

atau obrolan (chat) dukungan krisis online (24 jam sehari, 7 hari seminggu)

---

**Beyond Blue: 1300 22 4636 | [beyondblue.org.au](https://beyondblue.org.au)**

atau obrolan (chat) online (24 jam sehari, 7 hari seminggu)

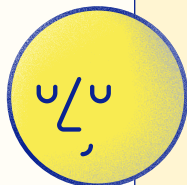
---

**Kids Helpline: 1800 55 1800 | [kidshelpline.com.au](https://kidshelpline.com.au)**

(24 jam sehari, 7 hari seminggu)

Dampak finansial dari penipuan dapat sangat menghancurkan dan mengubah hidup.

Jika Anda mengalami kesulitan keuangan, Anda dapat berbicara dengan konselor keuangan melalui **National Debt Helpline: 1800 007 007** dari 9:30am – 4:30pm Senin hingga Jumat or akses Live Chat dari pukul 9.00 – 20.00 Senin hingga Jumat



**[scamwatch.gov.au](https://scamwatch.gov.au)**